(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－188665
（P2001－188665A）
(43)公開日　平成13年７月10日(2001.7.10)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　3/12		Ｇ０６Ｆ　3/12	Ｋ	２Ｃ０６１
Ｂ４１Ｊ　29/38		Ｂ４１Ｊ　29/38	Ｚ	５Ｂ０２１
Ｇ０６Ｆ　13/00	３５４	Ｇ０６Ｆ　13/00	３５４Ｚ	５Ｂ０８５
15/00	３３０	15/00	３３０Ｂ	５Ｂ０８９

審査請求　未請求　請求項の数18　ＯＬ　（全 13 頁）

(21)出願番号　特願平11－374754

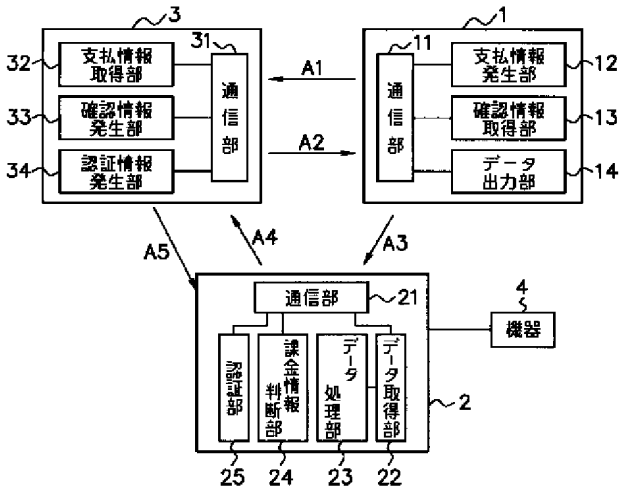
(22)出願日　平成11年12月28日(1999.12.28)

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号
(72)発明者　庄司　篤之
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内
(74)代理人　100090273
弁理士　國分　孝悦

Ｆターム(参考)　2C061 AP01 AP03 AP04 AP07 HJ08
HQ17 HX10
5B021 AA05 AA19 NN18
5B085 AC04 AE02 AE23 BG07
5B089 GA11 GA21 GB02 KA15 KA17
KB13 LB12

(54)【発明の名称】　ネットワークシステム、情報処理装置、情報処理方法、及びコンピュータ読み取り可能な記憶媒体

(57)【要約】
【課題】　不当な機器の利用に対して適当な処分を行うことで、機器管理者が経済的不利益をこうむることのない受益者負担のシステムを構築する。
【解決手段】　機器利用者側の情報処理装置１は、データを送信してネットワーク上の外部機器４を利用するとき、料金支払いに関する支払情報を電子マネーサーバ３に送信した上で、上記データに上記支払情報に基づく課金情報を添付して機器管理者側の情報処理装置２に送信する。機器管理者側の情報処理装置２では、上記機器利用者側の情報処理装置１から課金情報の添付されたデータを受信したとき、電子マネーサーバ３に対して当該課金情報についての認証要求を行う。そして、電子マネーサーバ３から正当な認証結果を得た場合は機器４の利用を許可し、課金情報が添付されていなかったり、認証結果で課金情報が正当なものでなかったりした場合は機器４を利用させない等の処分を行う。



【特許請求の範囲】
【請求項１】　ネットワークに接続された外部機器を利用するデータを送信する第１の情報処理装置と、上記外部機器を管理する第２の情報処理装置と、上記ネットワーク上での課金管理を行う第３の情報処理装置とを接続してなるネットワークシステムであって、
上記第１の情報処理装置は、上記外部機器を利用するとき、料金支払いに関する支払情報を上記第３の情報処理装置に送信した上で、上記データに上記支払情報に基づく課金情報を添付して上記第２の情報処理装置に送信し、
上記第２の情報処理装置は、上記第１の情報処理装置から上記課金情報の添付された上記データを受信したとき、上記第３の情報処理装置に対して上記課金情報についての認証要求を行う構成にしたことを特徴とするネットワークシステム。
【請求項２】　上記第３の情報処理装置は、上記第２の情報処理装置から上記認証要求があったとき、上記支払情報に基づく認証結果情報を返信することを特徴とする請求項１に記載のネットワークシステム。
【請求項３】　上記第２の情報処理装置は、上記第３の情報処理装置から受信した認証結果情報に応じて、上記受信したデータの処分を決めることを特徴とする請求項２に記載のネットワークシステム。
【請求項４】　上記第３の情報処理装置は、上記第１の情報処理装置から上記支払情報を受信したとき、確認情報を返信することを特徴とする請求項１に記載のネットワークシステム。
【請求項５】　外部との通信を行うための通信手段と、
上記通信手段を介してデータを受信するデータ取得手段と、
上記データ取得手段で受信したデータに課金情報が添付されているか否かを判断する課金情報判断手段と、
上記通信手段を介して上記課金情報についての認証要求を行う認証手段とを備えたことを特徴とする情報処理装置。
【請求項６】　上記認証要求により得られた認証結果に応じて、上記データ取得手段で受信した上記データの処分を決めることを特徴とする請求項５に記載の情報処理装置。
【請求項７】　上記認証手段により上記認証要求を行ってから上記認証結果を得るまでの待ち時間に上記データに所定の処理を施すことを特徴とする請求項５に記載の情報処理装置。
【請求項８】　上記データ取得手段で受信した上記データに応じて、上記通信手段を介して外部から必要なソフトウェアを取得するソフトウェア取得手段を備えたことを特徴とする請求項５に記載の情報処理装置。
【請求項９】　上記ソフトウェア取得手段は、上記認証手段により上記認証要求を行ってから上記認証結果を得るまでの待ち時間に上記ソフトウェアの取得を行うことを特徴とする請求項８に記載の情報処理装置。
【請求項１０】　ネットワークに接続された外部機器を利用するデータを送信する第１の情報処理装置と、上記外部機器を管理する第２の情報処理装置と、上記ネットワーク上での課金管理を行う第３の情報処理装置とを接続してなるネットワークシステムであって、
上記第１の情報処理装置は、上記外部機器を利用するとき、料金支払いに関する支払情報を上記第３の情報処理装置に送信して、上記データを上記第２の情報処理装置に送信し、
上記第３の情報処理装置は、上記第１の情報処理装置から上記支払情報を受信したとき、上記支払情報に基づく入金情報を上記第２の情報処理装置に送信し、
上記第２の情報処理装置は、上記第１の情報処理装置から上記データを受信し、上記第３の情報処理装置から上記入金情報を受信する構成にしたことを特徴とするネットワークシステム。
【請求項１１】　上記第１の情報処理装置から送信される上記データと、上記第３の情報処理装置から送信される上記入金情報とは互いに対応付けられていることを特徴とする請求項１０に記載のネットワークシステム。
【請求項１２】　外部との通信を行うための通信手段と、
上記通信手段を介してデータを受信するデータ取得手段と、
上記通信手段を介して入金情報を受信する入金情報取得手段と、
上記データ取得手段で受信した上記データと上記入金情報取得手段で受信した上記入金情報との対応付けを確認する確認手段とを備えたことを特徴とする情報処理装置。
【請求項１３】　上記データ取得手段で受信した上記データを保存する保存手段を備えたことを特徴とする請求項１２に記載の情報処理装置。
【請求項１４】　上記確認手段は、上記データ取得手段で受信したデータと上記入金情報取得手段で受信した入金情報との対応付けを、上記データ及び上記入金情報のそれぞれに付されたＩＤにより確認することを特徴とする請求項１２に記載の情報処理装置。
【請求項１５】　通信によりデータを受信するデータ取得手順と、
上記データ取得手順で受信した上記データに課金情報が添付されているか否かを判断する課金情報判断手順と、
通信により上記課金情報についての認証要求を行う認証手順とを有することを特徴とする情報処理方法。
【請求項１６】　通信によりデータを受信するデータ取得手順と、
通信により入金情報を受信する入金情報取得手順と、
上記データ取得手順で受信した上記データと上記入金情

報取得手順で受信した上記入金情報との対応付けを確認する確認手順とを有することを特徴とする情報処理方法。
【請求項１７】　通信によりデータを受信するデータ取得手順と、
上記データ取得手順で受信した上記データに課金情報が添付されているか否かを判断する課金情報判断手順と、通信により上記課金情報についての認証要求を行う認証手順とを実行するためのプログラムを記憶したことを特徴とするコンピュータ読み取り可能な記憶媒体。
【請求項１８】　通信によりデータを受信するデータ取得手順と、
通信により入金情報を受信する入金情報取得手順と、
上記データ取得手順で受信した上記データと上記入金情報取得手順で受信した上記入金情報との対応付けを確認する確認手順とを実行するためのプログラムを記憶したことを特徴とするコンピュータ読み取り可能な記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ネットワークシステム、情報処理装置、情報処理方法、及びコンピュータ読み取り可能な記憶媒体に関し、特にネットワーク上の機器の管理者と利用者とが離れているものに用いて好適なものである。
【０００２】
【従来の技術】一般に旧来のインターフェースは、装置間を物理的に固定接続してデータの送受を行うものであった。そのため、異なった装置とデータの送受を行う場合には、物理的に接続し直す必要があった。
【０００３】データの送受信を行う装置を変更するごとに物理的な接続を変更する手間を省くようにしたのがネットワークインターフェースである。ネットワークインターフェースによれば、従来は単体で使用されていた複写機や一の装置に一対一で接続されていたプリンタ等も、より高次な使用法が可能となる。例えば、デジタル複写機の印字機構をプリンタとして使用したり、デジタル複写機のスキャナ機構をコンピュータの画像読み取り装置として利用したりすることが可能となる。これは、複写機、プリンタ、ファクシミリ装置等の構成機構を個々に独立に扱えるようになったということであり、共通の機構を有するネットワーク接続されたこれら機器においては、運用上個々の機器の本質的差異が消失しつつある。
【０００４】これに対応するように、オフィスにおけるスペースの有効活用といった市場要求等から、ファクシミリ機能、複写機能、プリンタ機能、スキャナ機能等を一台に集積したマルチファンクションマシンが登場してきた。こうしたマルチファンクションマシンによれば、重複する機能を共通化することで、トータルのコストや設置面積の低減を図ることが可能となる。
【０００５】マルチファンクションマシンは、スモールオフィスにおいてはファクシミリ送信中にコピーが使えない等の不都合が生じることもあるが、ネットワーク環境下に複数台のマルチファンクションマシンが接続されている場合、最も効率よくハードウェアのリソースを使用することが可能となる。
【０００６】かかるマルチファンクションマシンとコンピュータ等をネットワークを介して相互接続して社内にローカルエリアネットワークを構築し、さらにセキュリティを司るファイアウォールを通じて社外のインターネットへと繋ぐことも一般的となってきている。このようなシステムでは、インターネットを介して遠方から画像データを送れば、従来のファクシミリとして使用することができる。
【０００７】
【発明が解決しようとする課題】上記従来例で述べたように広域ネットワークを利用する場合、機器管理者と機器利用者とが物理的に離れていることが一般的となる。
【０００８】現在でも、例えば電話回線を用いたファクシミリの利用においては、印字出力に使用されて消耗品を消費する機器と、その機器を利用する者とが離れていることにより、消耗品を使用する機器の管理者に一方的に経済的負担が押しつけられるといった不都合があった。このため、いたずらファックスにより用紙が無駄に使用されてしまったり、宣伝広告を一方的に押しつけられてしまったりする等のトラブルが後を絶たなかった。
【０００９】インターネット経由の情報量は従来の電話回線ファクシミリでの情報量よりも容易に膨大にすることができる。デジタル化されたデータはプログラムで生成したデータとスキャナで読み取った画像とを区別しないことからも、上記のようなトラブルの規模が大きくなってしまうことが容易に予想される。
【００１０】このため、インターネットと接続されたネットワーク下での不当な機器利用に対する適切な対策をとることが必要とされる。
【００１１】かかる対策をとるために、ローカルネットワークを外部に繋ぐインターネット上のファイアウォールを用いることも考えられるが、ファイアウォールは情報の不正な流出を防ぐことを基本的な目的としたものであり、情報の流入に対する判断は負担が大きくなり過ぎ、かつ、ネットワークの柔軟な利用を妨げることになり、ネットワーク自体のメリットを失わせることになりかねない。したがって、他の手法により、機器管理者と機器利用者との不一致による不都合を解消するための受益者負担のシステムを構築することが必要な状況となっている。
【００１２】本発明は、このような問題を解決するために成されたものであり、ネットワークの柔軟な利用を妨げることなく、受益者負担のシステムを構築することを

目的とする。
【００１３】
【課題を解決するための手段】本発明は上記の課題を解決するためになされたものであり、第１に、本発明のネットワークシステムは、ネットワークに接続された外部機器を利用するデータを送信する第１の情報処理装置と、上記外部機器を管理する第２の情報処理装置と、上記ネットワーク上での課金管理を行う第３の情報処理装置とを接続してなるネットワークシステムであって、上記第１の情報処理装置は、上記外部機器を利用するとき、料金支払いに関する支払情報を上記第３の情報処理装置に送信した上で、上記データに上記支払情報に基づく課金情報を添付して上記第２の情報処理装置に送信し、上記第２の情報処理装置は、上記第１の情報処理装置から上記課金情報の添付された上記データを受信したとき、上記第３の情報処理装置に対して上記課金情報についての認証要求を行う構成にした点に特徴を有する。
【００１４】第２に、上記第３の情報処理装置は、上記第２の情報処理装置から上記認証要求があったとき、上記支払情報に基づく認証結果情報を返信する点に特徴を有する。第３に、上記第２の情報処理装置は、上記第３の情報処理装置から受信した認証結果情報に応じて、上記受信したデータの処分を決める点に特徴を有する。第４に、上記第３の情報処理装置は、上記第１の情報処理装置から上記支払情報を受信したとき、確認情報を返信する点に特徴を有する。
【００１５】また、第５に、本発明の情報処理装置は、外部との通信を行うための通信手段と、上記通信手段を介してデータを受信するデータ取得手段と、上記データ取得手段で受信したデータに課金情報が添付されているか否かを判断する課金情報判断手段と、上記通信手段を介して上記課金情報についての認証要求を行う認証手段とを備えた点に特徴を有する。
【００１６】第６に、上記認証要求により得られた認証結果に応じて、上記データ取得手段で受信した上記データの処分を決める点に特徴を有する。第７に、上記認証手段により上記認証要求を行ってから上記認証結果を得るまでの待ち時間に上記データに所定の処理を施す点に特徴を有する。第８に、上記データ取得手段で受信した上記データに応じて、上記通信手段を介して外部から必要なソフトウェアを取得するソフトウェア取得手段を備えた点に特徴を有する。第９に、上記ソフトウェア取得手段は、上記認証手段により上記認証要求を行ってから上記認証結果を得るまでの待ち時間に上記ソフトウェアの取得を行う点に特徴を有する。
【００１７】また、第１０に、本発明のネットワークシステムは、ネットワークに接続された外部機器を利用するデータを送信する第１の情報処理装置と、上記外部機器を管理する第２の情報処理装置と、上記ネットワーク上での課金管理を行う第３の情報処理装置とを接続してなるネットワークシステムであって、上記第１の情報処理装置は、上記外部機器を利用するとき、料金支払いに関する支払情報を上記第３の情報処理装置に送信して、上記データを上記第２の情報処理装置に送信し、上記第３の情報処理装置は、上記第１の情報処理装置から上記支払情報を受信したとき、上記支払情報に基づく入金情報を上記第２の情報処理装置に送信し、上記第２の情報処理装置は、上記第１の情報処理装置から上記データを受信し、上記第３の情報処理装置から上記入金情報を受信する構成にした点に特徴を有する。
【００１８】第１１に、上記第１の情報処理装置から送信される上記データと、上記第３の情報処理装置から送信される上記入金情報とは互いに対応付けられている点に特徴を有する。
【００１９】また、第１２に、本発明の情報処理装置は、外部との通信を行うための通信手段と、上記通信手段を介してデータを受信するデータ取得手段と、上記通信手段を介して入金情報を受信する入金情報取得手段と、上記データ取得手段で受信した上記データと上記入金情報取得手段で受信した上記入金情報との対応付けを確認する確認手段とを備えた点に特徴を有する。
【００２０】第１３に、上記データ取得手段で受信した上記データを保存する保存手段を備えた点に特徴を有する。第１４に、上記確認手段は、上記データ取得手段で受信したデータと上記入金情報取得手段で受信した入金情報との対応付けを、上記データ及び上記入金情報のそれぞれに付されたＩＤにより確認する点に特徴を有する。
【００２１】また、第１５に、本発明の情報処理方法は、通信によりデータを受信するデータ取得手順と、上記データ取得手順で受信した上記データに課金情報が添付されているか否かを判断する課金情報判断手順と、通信により上記課金情報についての認証要求を行う認証手順とを有する点に特徴を有する。
【００２２】第１６に、本発明の情報処理方法は、通信によりデータを受信するデータ取得手順と、通信により入金情報を受信する入金情報取得手順と、上記データ取得手順で受信した上記データと上記入金情報取得手順で受信した上記入金情報との対応付けを確認する確認手順とを有する点に特徴を有する。
【００２３】また、第１７に、本発明のコンピュータ読み取り可能な記憶媒体は、通信によりデータを受信するデータ取得手順と、上記データ取得手順で受信した上記データに課金情報が添付されているか否かを判断する課金情報判断手順と、通信により上記課金情報についての認証要求を行う認証手順とを実行するためのプログラムを記憶した点に特徴を有する。
【００２４】第１８に、本発明のコンピュータ読み取り可能な記憶媒体は、通信によりデータを受信するデータ取得手順と、通信により入金情報を受信する入金情報取

得手順と、上記データ取得手順で受信した上記データと上記入金情報取得手順で受信した上記入金情報との対応付けを確認する確認手順とを実行するためのプログラムを記憶した点に特徴を有する。

【００２５】上記のようにした本発明では、外部から受信したデータに課金情報が添付されていなかったり、課金情報が正当なものでなかったりした場合、又は、外部から受信したデータに対応する入金情報がない場合に、機器を利用させない等の処分を行うことが可能となり、不当な機器利用に対する適切な対策をとることができる。

【００２６】

【発明の実施の形態】以下、本発明の実施の形態を図面に基づいて説明する。

（第１の実施の形態）図１には、第１の実施の形態のネットワークシステムの概要を示す。このネットワークシステムでは、外部機器４を利用するデータを送信する機器利用者側の情報処理装置１と、上記外部機器４を管理する機器管理者側の情報処理装置２と、ネットワーク上での課金管理を行う情報処理装置３とを具備し、インターネット等の通信網を介して互いに接続している。

【００２７】機器利用者側の情報処理装置１は、通信網に接続するための通信部１１と、情報処理装置３に支払情報を送信する支払情報発生部１２と、情報処理装置３から確認情報を受信する確認情報取得部１３と、機器管理者側の情報処理装置２に上記支払情報に基づく課金情報を添付したデータを送信するデータ出力部１４とを有する。

【００２８】機器管理者側の情報処理装置２は、通信網に接続するための通信部２１と、機器利用者側の情報処理装置１からデータを受信するデータ取得部２２と、データ取得部２２で受信したデータに機器４を利用するための処理を施すデータ処理部２３と、データ取得部２２で受信したデータに課金情報が添付されている否かを判断する課金情報判断部２４と、情報処理装置３に課金情報についての認証要求を行う認証部２５とを有する。なお、この情報処理装置２は、機器４と別に設けられたものであってもよいし、機器４に内蔵されたものであってもよい。

【００２９】課金管理用の情報処理装置３は、通信網に接続するための通信部３１と、機器利用者側の情報処理装置１から支払情報を受信する支払情報取得部３２と、支払情報についての確認情報を返信する確認情報発生部３３と、機器管理者側の情報処理装置２から認証要求があったとき認証結果情報を返信する認証情報発生部３４とを有する。この課金管理用の情報処理装置３としては、後からも述べるが、銀行等の金融機関と消費者クライアントとの間の決済処理等を行う電子マネーサーバ等が用いられる。

【００３０】例えば、機器利用者は、画像データを送って外部機器４を利用しようとする場合、まず課金管理用の情報処理装置３に支払情報を送信する（図中矢印Ａ１）。支払情報は、機器管理者への料金支払いに関する情報であり、自己の保有する金額からいくら支払うかの情報（支払い額情報）が含まれる。この支払情報は、第三者への漏洩を防止するために暗号化する等して情報処理装置３に送信される。

【００３１】課金管理用の情報処理装置３は、上記支払情報を受信したならば、確認のための確認情報を機器利用者側の情報処理装置１に送信する（図中矢印Ａ２）。なお、支払情報は暗号化されているので情報処理装置３側での解読用の鍵が必要となるが、これは銀行の口座でいえば出金時の暗証番号に相当する。

【００３２】機器利用者側の情報処理装置１は、課金管理用の情報処理装置３から確認情報を受信したならば、上記支払情報に基づく課金情報を添付した画像データを機器管理者側の情報処理装置２に送信する（図中矢印Ａ３）。この課金情報とは、必要な額の支払い能力があり、機器管理者に対して料金を支払う意志があることを示すもので、少なくとも、料金を支払う者（機器利用者）、料金を受け取る者（機器管理者）、支払い金額の３項目を含んでいる。これら全ての情報も、第三者への漏洩を防止するよう保護されていなければならない。また、ネットワーク上には課金管理用の情報処理装置３が１つだけとは限らず、課金情報の認証先を特定する必要があることから、当該課金情報には、どこに問い合わせるかについての情報も含まれている。

【００３３】機器管理者側の情報処理装置２では、機器利用者側から課金情報の添付された画像データを受信したならば、課金管理用の情報処理装置３に対してその課金情報についての認証要求を行う（図中矢印Ａ４）。

【００３４】課金管理用の情報処理装置３では、機器管理者側からの認証要求があったならば、事前に機器利用者側から支払情報のあったものかどうかを確認し、正当なものか否かの認証を行うべく機器管理者側の情報処理装置２に認証結果情報を送信する（図中矢印Ａ５）。

【００３５】機器管理者側の情報処理装置２では、課金情報が正当なものであるとの認証情報を得た場合は、機器４の利用を許可する。それに対して、課金情報が添付されていなかったり、課金情報が正当なものでなかったりした場合は、機器４を利用させない等の処分を行うことで、不当な機器利用に対する適切な対策をとることができる。

【００３６】なお、機器利用者が課金管理用の情報処理装置３に課金情報と画像データとを送信し、それを機器管理者側の情報処理装置２に転送してもらうといった手法も考えられる。しかし、画像データが長大な情報量となることもあり、このような画像データが課金情報とともに送信されてくると、課金管理用の情報処理装置３の負担が増大し過ぎることも予想される。そこで、本実施

の形態では、上述のように、機器利用者側の情報処理装置１は、課金管理用の情報処理装置３に支払情報のみを送信した上で、機器管理者側の情報処理装置２に課金情報を添付した画像データを直接送信するようにしている。

【００３７】ここまで述べた課金管理はいわゆる預金方式によるが、課金管理用の情報処理装置３への事前の支払い額確認を簡略化したクレジットカード方式をとることも可能である。この場合は、機器利用者側から課金管理用の情報処理装置３へ事前に支払情報を送る必要がないが、機器管理者側からの不当な金額要求等のトラブルに対応できないので、支払額に限度を設定する等の現行のクレジットカードで実施されているような対策が必要となる。

【００３８】図２は、ネットワークシステムの一具体例を示す図である。１００はインターネット等の通信網である。２００はウェブサーバであり、インターネットユーザに特定のサービスを提供する。

【００３９】３００は電子マネーサーバであり、銀行等の金融機関と消費者クライアントとの間の決済処理等を行う。４００はサービスプロバイダであり、個人ユーザの端末とインターネット１００との接続処理を行う。５００はファイアウォールであり、ＬＡＮと外部通信網であるインターネット１００とを接続し、セキュリティ管理等を行う。

【００４０】ＬＡＮにおいて、６００は機器管理サーバであり、ＬＡＮ上に接続された各機器７００～１０００の管理、ユーザ管理、課金情報等のデータ管理等を行う。７００はファイルサーバであり、広告データの管理等を行う。８００はマルチファンクションマシンであり、詳しくは後述するが、主に画像データの入出力等の機能を有する。

【００４１】９００はプリンタであり、パーソナルコンピュータ１０００やフィルサーバ７００からの画像データを記録媒体上にプリントする。１０００は端末装置として接続されたパーソナルコンピュータであり、インターネット１００を介してウェブサーバ２００から提供された情報を閲覧したり、画像データをマルチファンクションマシン８００やプリンタ９００に出力したりする。なお、上記マルチファンクションマシン８００やプリンタ９００が、図１で説明した機器４に相当するものである。

【００４２】上記マルチファンクションマシン８００は、ユーザが操作するための操作部８１０、操作部８１０やパーソナルコンピュータ１０００からの指示に従って画像を入力するためのイメージスキャナ８２０、パーソナルコンピュータ１０００やファイルサーバ７００からのデータを印刷するプリンタ８３０、デバイスコントローラ８４０、メモリ８５０、ハードディスク８６０から構成される。

【００４３】このようにしたマルチファンクションマシン８００において、上記デバイスコントローラ８４０は、操作部８１０やパーソナルコンピュータ１０００からの指示に従って、イメージスキャナ８２０、プリンタ８３０、メモリ８５０やハードディスク８６０、パーソナルコンピュータ１０００の間で画像データの入出力等の制御を行う。例えば、イメージスキャナ８２０により読み込んだ画像データをメモリ８５０やハードディスク８６０に必要に応じて蓄積したり、パーソナルコンピュータ１０００に出力したり、あるいはプリンタ８３０で印刷したりする等の制御を行う。このデバイスコントローラ８４０は、ハードウェアの描画機構及びＣＰＵと実行ソフトウェアによって構成される。

【００４４】なお、図面上においてファイアウォール５００より下方に示したＬＡＮ構成は、サービスプロバイダ４００を介してインターネットに繋がっている個人ユーザのもとにあってもよい。

【００４５】次に、インターネット経由で、遠方のユーザからファクシミリ情報又は印字出力要求を伴うイメージ情報（以下、データという）がＬＡＮに送られてきたときの動作を説明する。

【００４６】遠方のユーザは、マルチファンクションマシン８００やプリンタ９００を正当な課金負担の下で意図する出力を実行して利用するのであれば、既に説明したように、送信するデータに適切な課金情報を添付する。

【００４７】以下、図３のフローチャートを用いて、遠方のユーザからデータが送られてきたときのマルチファンクションマシン８００やプリンタ９００側での処理を説明する。ステップＳ１０１で、インターネット等の通信網１００を経由したデータ（データパケット）を受信したならば、ステップＳ１０２で、そのデータに課金情報が添付されているか否かを確認する。

【００４８】ステップＳ１０２において課金情報が添付されていれば、ステップＳ１０３で認証パケットを送出し、電子マネーサーバ３００に対して当該課金情報についての認証要求を行う。また、ステップＳ１０４でデータ処理を開始して出力イメージを生成し、ステップＳ１０５で出力イメージを生成した状態で電子マネーサーバ３００からの認証を待機する。

【００４９】そして、電子マネーサーバ３００から認証結果情報の返信があったならば、ステップＳ１０６で上記課金情報が正当なものであるか否かを判定し、正当なものであれば、既に生成した出力イメージについて印字出力を実行する（ステップＳ１０７）。すなわち、正当な課金情報を添付してきたユーザに対しては機器を利用させることとなる。ステップＳ１０６の判定において課金情報が正当なものでないと判定された場合は、後述するステップＳ１１２に移る。

【００５０】なお、課金情報についての認証を行う際

に、情報隠蔽手段が用意されていないインターネット等のネットワーク上に情報を流すのは問題がある。したがって、課金情報の認証には、十分な暗号化を施すか、あるいは専用線を使用することによって実施するのが望ましい。ローカルネットワークを課金情報のために二重化するのが現実的でない場合は、ファイアウォール５００内は暗号化によって、電子マネーサーバ３００までは専用線を使用することによって等の運用上の使い分けを行えばよい。

【００５１】一方、上記ステップＳ１０２において課金情報が添付されていなければ、ステップＳ１０８でユーザ情報確認パケットを送出し、ローカルサーバ（機器管理サーバ６００）に機器利用者に関するユーザ情報を確認する。また、ステップＳ１０９でデータ処理を開始してイメージ出力を生成し、ステップＳ１１０で出力イメージを生成した状態でローカルサーバからのユーザ情報を待機する。

【００５２】そして、ローカルサーバからユーザ情報が送られてきたら、ステップＳ１１１で、データの送信元が信用に値するとして登録されているユーザであるかどうかを判定する。信用に値するとして登録されているとのユーザ情報が得られれば、ステップＳ１０７に移って、既に生成した出力イメージについて印字出力を行う。すなわち、データに課金情報が添付されていなかった場合でも、特定のユーザに対しては機器を利用させることとなる。ステップＳ１１１の判定において登録もされていないユーザであるとのユーザ情報が得られた場合は、後述するステップＳ１１２に移る。

【００５３】ステップＳ１１２、Ｓ１１３では、正当でない課金情報が添付されていたデータ（ステップＳ１０６）、あるいは、課金情報が添付されずユーザ登録もないデータ（ステップＳ１１１）についての処分が決定される。本実施の形態では、仮出力モード、情報保存モード、破棄モードといった３つのモードが設定され、機器管理者側の設定に応じていずれかのモードが選択される。

【００５４】仮出力モードに設定されていた場合、正当でない課金情報が添付されていたデータ、あるいは、課金情報が添付されずユーザ登録もないデータについても印字出力を行う（ステップＳ１１４～Ｓ１１６）。ただし、ステップＳ１１５で出力用紙を切り替えて廉価な用紙を選択した上で、ステップＳ１１６で印字出力を行うようにしている。そのため、ステップＳ１１４においては、既に生成されている出力イメージのリサンプル、変換処理を行っている。なお、廉価な用紙を使用する以外にも、縮小印刷とする、省トナー印字を行う、カラー印刷をモノクロで代用する等の廉価な印字モードにより出力を行うようにしてもよい。

【００５５】また、情報保存モードに設定されていた場合、既に生成されている出力イメージを、マルチファクションマシン８００やプリンタ９００、外部のパーソナルコンピュータ１０００、機器管理サーバ６００等に転送して保存する（ステップＳ１１７）。これにより、機器管理者は、データの内容を確認した上で、印字出力するか、あるいは、データを破棄するかを判断することが可能となる。

【００５６】また、破棄モードに設定されている場合、既に生成されている出力イメージを破棄する（ステップＳ１１８）。つまり、正当でない課金情報が添付されていたデータ、あるいは、課金情報が添付されずユーザ登録もないデータについては、印字出力を一切拒否することになる。

【００５７】以上述べた第１の実施の形態によれば、正当な料金を支払うユーザには機器を利用させるとともに、不当な利用に対しては適当なデータの処分を行うことで、機器管理者が経済的不利益をこうむることのない受益者負担のシステムを構築することができる。

【００５８】（第２の実施の形態）多くの入出力機構を備えるマルチファンクションマシンにおいては、要求される画像処理パターンは多岐にわたり、扱うデータフォーマットも多くなる。これら全てに対応するプログラムを単体に実装、製品化することには、かなりのコストが見込まれる。また、新規フォーマット、新規の画像処理処理パターンに対するアップデート作業も大変なものとなる。

【００５９】ネットワークに接続されることを前提とするマルチファクションマシンにおいては、必要最小限の機能のみを実装し、必要なソフトウェアはその都度サーバ等から取得し、実行するという機器構成をとるといった選択肢がある。このような機器構成によるメリットは、マルチファンクションマシン単体の記憶容量等のコストを下げることができ、また、ソフトウェアのアップデートも容易となることである。さらに、ソフトウェアのアップデートが容易であることによって、個別機器の物理的リプレースなしで新規に設定されたデータフォーマットにも対応が可能となる。

【００６０】なお、デメリットとしては、ネットワークやサーバにトラブルが発生し情報のやり取りができなくなった場合に、単体では多くの処理が行えなくなることが挙げられる。しかし、もともとネットワークやサーバにトラブルが発生した場合は、マルチファンクションマシンのプリンタやファクシミリとしての使用は不可能となることから、多くの機能において上記のデメリットは無視しうるものといえる。

【００６１】そこで、本実施の形態では、ネットワーク間の情報の入出力を主体としたマルチファンクションマシンにおいては、必要なソフトウェアはその都度サーバ等から取得し、実行するという機器構成をとることにしている。

【００６２】ここで、上記第１の実施の形態で述べたよ

うに、機器管理者側では、課金情報の正当性を確認するために、電子マネーサーバ３００との間で認証のやり取りを行わなければならない。図２でいえば、ＬＡＮ内部とＬＡＮ外部との情報のやり取りを行う必要があることから、タイムラグが生じ、認証結果情報を得るまでの待ち時間ができる公算が大きい。

【００６３】そこで、本実施の形態では、この待ち時間を、ローカルサーバからの必要なアプリケーションのダウンロード時間として利用することにしている。以下、図４のフローチャートを用いて、第２の実施の形態での処理を説明する。なお、本第２の実施の形態の構成としては、データの受信機構、課金情報の確認機構をデフォルトとして個別機器に格納する。

【００６４】ステップＳ２０１で、インターネット等の通信網１００を経由したデータ（データパケット）を受信したならば、ステップＳ２０２で認証パケットを送出し、電子マネーサーバ３００に対して当該課金情報についての認証要求を行う。

【００６５】また、ステップＳ２０３で受信したデータのデータフォーマットを解析し、ステップＳ２０４で、内蔵するプログラムによるデータ処理が可能か否かを判断する。

【００６６】上記ステップＳ２０４において対応する内蔵プログラムでの処理ができないと判断されたならば、ステップＳ２０５で、ローカルサーバに対して必要なアプリケーションの転送を要求する。そして、アプリケーションの転送を待って（ステップＳ２０６）、転送が終了したならば（ステップＳ２０７）、ステップＳ２０８でデータ処理を開始して出力イメージを生成し、ステップＳ２０９で出力イメージを生成した状態で電子マネーサーバ３００からの認証を待機する。

【００６７】そして、電子マネーサーバ３００から認証結果情報の返信があったならば、ステップＳ２１０で上記課金情報が正当なものであるか否かを判定し、正当なものであれば、既に生成した出力イメージについて印字出力を行う（ステップＳ２１１）。

【００６８】なお、上記ステップＳ２０４において対応する内蔵プログラムがあると判断されれば、ソフトウェアをダウンロードする必要はないので、そのままステップＳ２０８に移る。

【００６９】アプリケーションの転送が規定時間を超えてもなされない場合（ステップＳ２１２）や、課金情報が正当なものでないとの認証結果が得られた場合（ステップＳ２１０）、ステップＳ２１３に移って例外処理を行う。

【００７０】以上説明した図４においては、表記上フローチャートとして記述しているが、電子マネーサーバ３００からの認証待ちと、アプリケーションの受信及びデータ処理とは並列に実行される必要がある。そして、実際にどちらかを「待つ」のは、いずれか一方の処理が全て終わった時点での話である。例えば、データ処理の終了前に課金情報が正当である旨の認証結果を得た場合、そのデータ処理を継続する。データ処理の終了前に課金情報が正当でない旨の認証結果を得た場合は、データ処理をその時点でキャンセルする。

【００７１】アプリケーションとしては、例えばデータフォーマットが付加されている使用要求に対しては、データフォーマットごとにアプリケーションもしくはアプリケーションのモジュールを用意してもよい。この場合、データフォーマットをローカルサーバに通知し、対応するアプリケーションやモジュール等を受け取り実行する。

【００７２】（第３の実施の形態）上記第１の実施の形態では、図１に示す矢印Ａ１～Ａ５で説明したような手順をとるようにしたが、機器利用者は課金管理用の情報処理装置３からの確認情報を待つ必要があり（図中矢印Ａ２）、また、機器管理者は課金管理用の情報処理装置３に認証要求を行って認証を待機する必要があることから（図中矢印Ａ４、Ａ５）、待ち時間が生じてしまう。

【００７３】そこで、本第３の実施の形態では、図５に示すようにして情報のやり取りを行うようにしている。

【００７４】機器利用者側の情報処理装置１は、通信網に接続するための通信部１５と、情報処理装置３に支払情報を送信する支払情報発生部１６と、機器管理者側の情報処理装置２にＩＤを付したデータを送信するデータ出力部１７とを有する。

【００７５】機器管理者側の情報処理装置２は、通信網に接続するための通信部２６と、機器利用者側の情報処理装置１からデータを受信するデータ取得部２７と、データ取得部２７で受信したデータに機器４を利用するための処理を施すデータ処理部２８と、課金管理用の情報処理装置３から入金情報を受信する入金情報取得部２９と、上記入金情報に付されたＩＤと上記データに付されたＩＤとの対応付けを確認するＩＤ確認部３０とを有する。

【００７６】課金管理用の情報処理装置３は、通信網に接続するための通信部３５と、機器利用者側の情報処理装置１から支払情報を受信する支払情報取得部３６と、機器管理者側の情報処理装置２に入金情報を送信する入金情報発生部３７とを有する。上記入金情報は、支払情報取得部３６で受信した支払情報に基づくもので、ＩＤが付された状態で機器管理者側の情報処理装置２に送信される。この課金管理用の情報処理装置３としては、前述のように、銀行等の金融機関と消費者クライアントとの間の決済処理等を行う電子マネーサーバ等が用いられる。

【００７７】例えば、機器利用者は、画像データを送って外部機器４を利用しようとする場合、まず機器管理用の情報処理装置３に支払情報を送信する（図中矢印Ｂ１）。支払情報は、機器管理者への料金支払いに関する

情報であり、自己の保有する金額からいくら支払うかの情報（支払い額情報）が含まれる。

【００７８】また、機器利用者は、機器管理者側の情報処理装置２に、所定のＩＤを含ませた画像データを送信する（図中矢印Ｂ２）。

【００７９】課金管理用の情報処理装置３は、上記支払情報を受信したならば、その支払情報に基づく入金情報を機器管理者側の情報処理装置２に送信する（図中矢印Ｂ３）。この入金情報は、機器利用者側からの支払いがある旨を伝える情報であり、所定のＩＤを含ませた状態で送信される。

【００８０】機器管理者側の情報処理装置２は、機器利用者側から画像データを受信し、また、課金管理用の情報処理装置３から入金情報を受信したならば、これら画像データ及び入金情報に付されているＩＤを確認して、互いに対応するものかどうかを判断する。そして、画像データと入金情報とが対応するものであれば、機器４の利用を許可する。それに対して、画像データに対応する入金情報の受信がないような場合は、機器４を利用させない等の処分を行うことで、不当な機器利用に対する適切な対策をとることができる。

【００８１】この第３の実施の形態でも、図２に示したネットワークシステムに基づいて、インターネットを経由したデータ及び入金情報がＬＡＮに送られてきたときの動作を説明する。図６は、データ及び入金情報が送られてきたときのマルチファンクションマシン８００やプリンタ９００側での処理を説明するためのフローチャートである。本実施の形態では、マルチファンクションマシン８００やプリンタ９００側に入金情報とデータとが別々に送られてくるので、２つの独立したフローチャートにより処理が行われる。

【００８２】図６（ａ）は、データを受信したときの処理を示す。ステップＳ３０１で、インターネット等の通信網１００を経由したデータ（データパケット）を受信したならば、ステップＳ３０２でデータ処理を開始し、ステップＳ３０３で出力イメージを生成する。

【００８３】そして、ローカルサーバ（機器管理サーバ６００）に機器利用者に関するユーザ情報を確認し、ステップＳ３０４で、データの送信元が信用に値するとして登録されているユーザであるかどうかを判定する。

【００８４】信用に値するとして登録されているとのユーザ情報が得られれば、ステップＳ３０４に移って、既に生成した出力イメージについて印字出力を行う。すなわち、特定のユーザに対しては、データが送られてきた時点で機器を利用させる。

【００８５】登録もされていないユーザであるとのユーザ情報が得られた場合は、ステップＳ３０６に移って、出力イメージをハードディスク８６０に保存しておく。データと入金情報とは別々に送られてくることから、データに遅れて入金情報が送られてくることも多く、その場合に、入金情報の遅れで重要な情報が破棄されるのを防ぐためである。

【００８６】図６（ｂ）は、入金情報を受信したときの処理を示す。インターネット等の通信網１００を経由して入金情報を受信したならば、ステップＳ３０７で、ハードディスク８６０に保存されたイメージ出力（図６（ａ）のステップＳ３０６）の順次読み出しを開始する。そして、ステップＳ３０８で、保存されているイメージ出力があるかどうかを判定する。

【００８７】保存されているイメージ出力がある場合、ステップＳ３０９に移って、そのイメージ出力についてのＩＤ（データに付されていたＩＤ）を、入金情報に付されたＩＤと比較する。そして、両ＩＤが一致するものであれば（ステップＳ３１０）、すなわち、データと入金情報とが対応するものであれば、ステップＳ３１１で当該出力イメージについて印字出力を行う。印字出力の終えた出力イメージはハードディスク８６０から消去して破棄する（ステップＳ３１２）。なお、両ＩＤが一致しなければ（ステップＳ３１０）、順次別データを読み出すようにして（ステップＳ３１３）、入金情報に対応する出力イメージを探し出す。

【００８８】ステップＳ３０８においてイメージ出力がなければ、ステップＳ３１４に移って、入金情報に対応するデータがないとして終了する。

【００８９】図７のフローチャートには、データのみが送信されて入金情報がない場合に、ハードディスク８６０に保存されている当該データの出力イメージを破棄するための処理を示す。

【００９０】図６（ａ）で述べたように、受信したデータの出力イメージをハードディスク８６０に保存して入金情報の受信を待機するが、ある程度の時間が経っても未だ入金情報が送られてこない場合は、不当に機器を利用しようとするものと考えられる。この場合には、ハードディスク８６０の空き容量を確保するためにも、不要な情報を削除する必要がある。なお、このフローチャートは、例えば１日に１回、日付の変化に合わせて起動するようにしておけばよい。

【００９１】ステップＳ３１５では、ハードディスク８６０に保存されているイメージ出力の順次読み出しを開始する。そして、ステップＳ３１６で、保存されているイメージ出力があるかどうかを判定する。

【００９２】保存されているイメージ出力がある場合、ステップＳ３１７でその登録日時を確認し、ステップＳ３１８では、保存されてから現在までの時間が予め設定されている規定時間を超過しているか否かを判断する。

【００９３】そして、規定時間を超過していれば、対応する入金情報の受信はもうないものと考えられるので、ステップＳ３１９に移って、そのイメージ出力を不要なものとしてハードディスク８６０から削除する。

【００９４】このようにしてハードディスク８６０に保

存されている全ての出力イメージについて判断して（ステップＳ３２０）、このフローチャートを終了する。

【００９５】以上述べた第３の実施の形態によれば、機器管理用の情報処理装置３（電子マネーサーバ３００）から機器管理者側に直接に入金情報を送るようにしたので、機器利用者は確認情報を待つ必要がなく、また、機器管理者は認証要求を行い認証結果を待つ必要がなくなり、ネットワーク上のトラフィック及び待ち時間を解消することができる。

【００９６】（その他の実施の形態）本発明は複数の機器（例えば、ホストコンピュータ、インターフェース機器、リーダ、プリンタ等）から構成されるシステムに適用しても１つの機器（例えば、複写機、ファクシミリ装置）からなる装置に適用してもよい。

【００９７】また、上述した実施の形態の機能を実現するべく各種のデバイスを動作させるように、該各種デバイスと接続された装置あるいはシステム内のコンピュータに対し、上記実施の形態の機能を実現するためのソフトウェアのプログラムコードを供給し、そのシステムあるいは装置のコンピュータ（ＣＰＵあるいはＭＰＵ）に格納されたプログラムに従って上記各種デバイスを動作させることによって実施したものも、本発明の範疇に含まれる。

【００９８】また、この場合、上記ソフトウェアのプログラムコード自体が上述した実施の形態の機能を実現することになり、そのプログラムコード自体、およびそのプログラムコードをコンピュータに供給するための手段、例えばかかるプログラムコードを格納した記録媒体は本発明を構成する。かかるプログラムコードを記憶する記録媒体としては、例えばフロッピーディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、磁気テープ、不揮発性のメモリカード、ＲＯＭ等を用いることができる。

【００９９】また、コンピュータが供給されたプログラムコードを実行することにより、上述の実施の形態の機能が実現されるだけでなく、そのプログラムコードがコンピュータにおいて稼働しているＯＳ（オペレーティングシステム）あるいは他のアプリケーションソフト等と共同して上述の実施の形態の機能が実現される場合にもかかるプログラムコードは本発明の実施の形態に含まれることは言うまでもない。

【０１００】さらに、供給されたプログラムコードがコンピュータの機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその機能拡張ボードや機能拡張ユニットに備わるＣＰＵ等が実際の処理の一部又は全部を行い、その処理によって上述した実施の形態の機能が実現される場合にも本発明に含まれることは言うまでもない。

【０１０１】なお、上記実施の形態において示した各部の形状及び構造は、何れも本発明を実施するにあたっての具体化のほんの一例を示したものに過ぎず、これらによって本発明の技術的範囲が限定的に解釈されてはならないものである。すなわち、本発明はその精神、又はその主要な特徴から逸脱することなく、様々な形で実施することができる。

【０１０２】

【発明の効果】以上説明したように本発明によれば、正当な料金を支払うユーザには機器を利用させるとともに、不当な利用に対してはデータに適当な処分を行うことで、機器管理者が経済的不利益をこうむることのない受益者負担のシステムを構築することができる。

【図面の簡単な説明】

【図１】第１の実施の形態のネットワークシステムを示す概要図である。

【図２】ネットワークシステムの具体例を示す図である。

【図３】第１の実施の形態においてインターネットを経由してデータが送信されてきたときの処理を示すフローチャートである。

【図４】第２の実施の形態での処理を説明するためのフローチャートである。

【図５】第３の実施の形態のネットワークシステムを示す概要図である。

【図６】第３の実施の形態においてインターネットを経由してデータ及び入金情報が送信されてきたときの処理を示すフローチャートである。

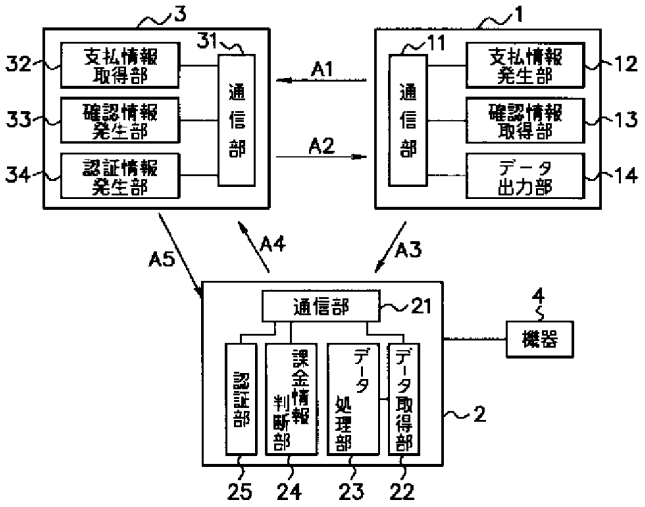
【図７】データのみが送信されて入金情報がない場合に、保存されている当該データの出力イメージを破棄するための処理を示すフローチャートである。

【符号の説明】

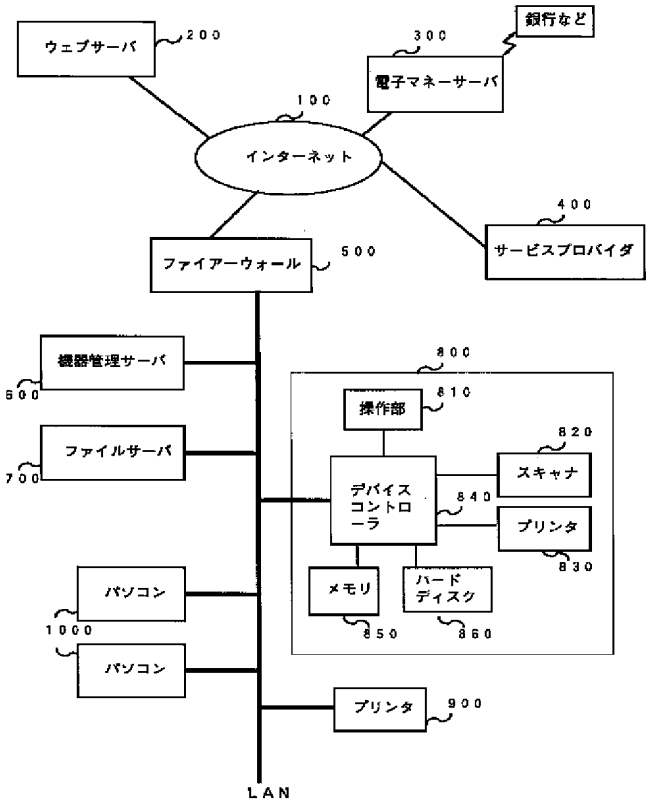
１	機器利用者側の情報処理装置
２	機器管理者側の情報処理装置
３	課金管理用の情報処理装置
４	外部機器
１１、１５	通信部
１２、１６	支払情報発生部
１３	確認情報取得部
１４、１７	データ出力部
２１、２６	通信部
２２、２７	データ取得部
２３、２８	データ処理部
２４	課金情報判断部
２５	認証部
２９	入金情報取得部
３０	ＩＤ確認部
３１、３５	通信部
３２、３６	支払情報取得部
３３	確認情報発生部
３４	認証情報発生部

３７	入金情報発生部
１００	インターネット等の通信網
２００	ウェブサーバ
３００	電子マネーサーバ
４００	サービスプロバイダ
５００	ファイアウォール
６００	機器管理サーバ
７００	ファイルサーバ
８００	マルチファンクションマシン
９００	プリンタ
１０００	パーソナルコンピュータ
８１０	操作部
８２０	イメージスキャナ
８３０	プリンタ
８４０	デバイスコントローラ
８５０	メモリ
８６０	ハードディスク

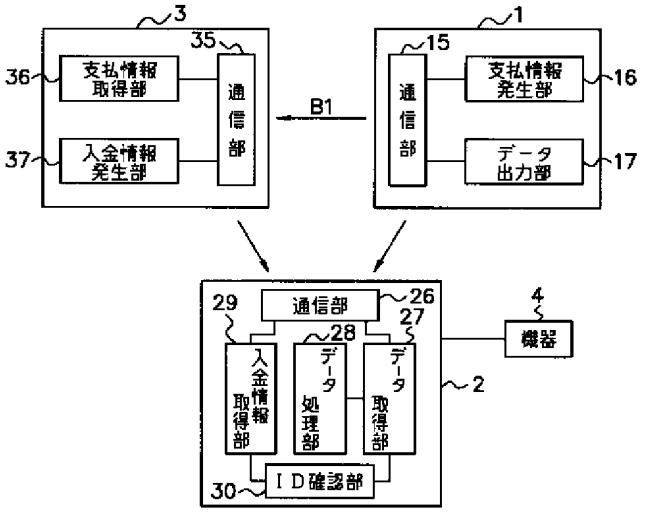
【図１】



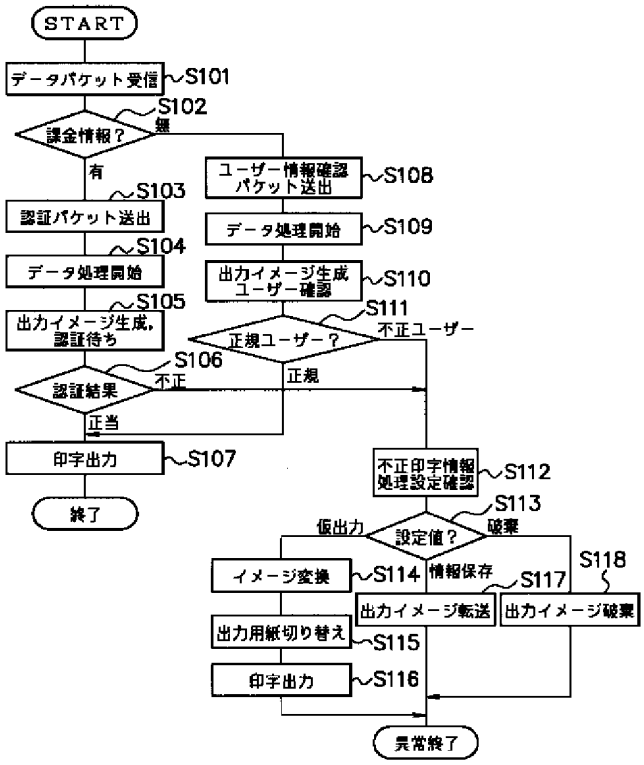
【図２】



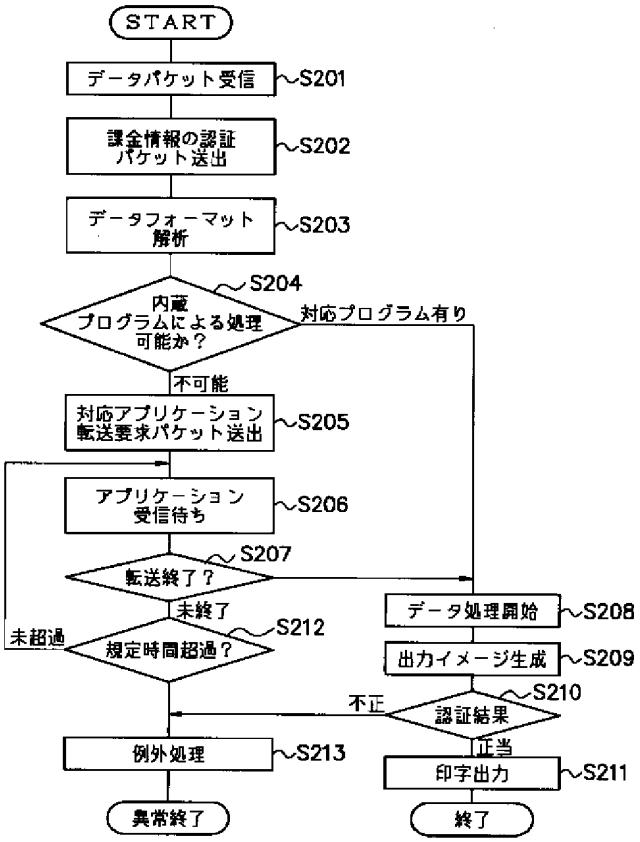
【図５】



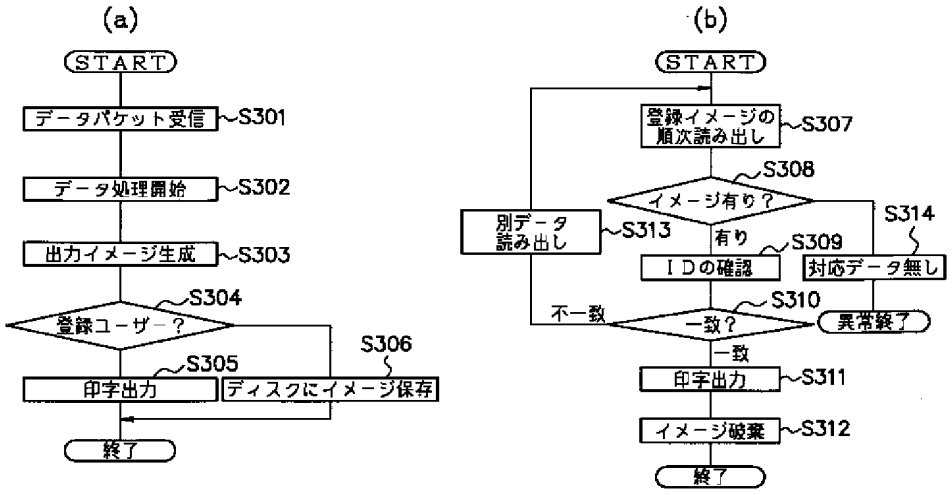
【図３】


START
データパケット受信
S101
課金情報？
S102
無
有
S103
認証パケット送出
S104
データ処理開始
S105
出力イメージ生成，認証待ち
S106
認証結果
不正
正当
印字出力
S107
終了
ユーザー情報確認パケット送出
S108
データ処理開始
S109
出力イメージ生成ユーザー確認
S110
S111
正規ユーザー？
不正ユーザー
正規
不正印字情報処理設定確認
S112
S113
仮出力
設定値？
破棄
イメージ変換
S114
情報保存
S117
S118
出力イメージ転送
出力イメージ破棄
出力用紙切り替え
S115
印字出力
S116
異常終了

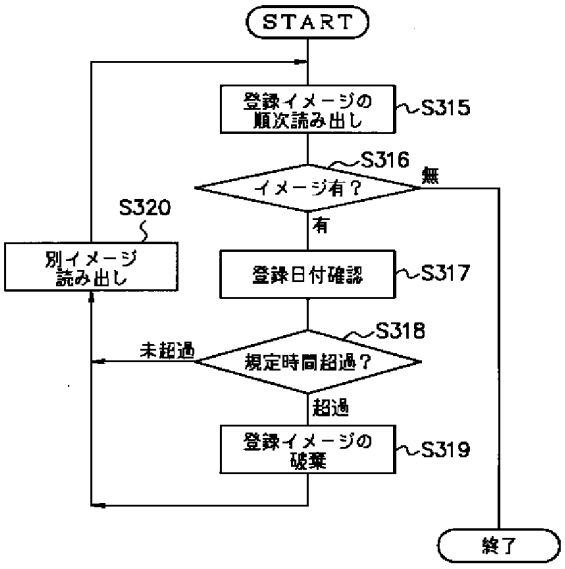
【図４】


START
データパケット受信
S201
課金情報の認証パケット送出
S202
データフォーマット解析
S203
S204
内蔵プログラムによる処理可能か？
対応プログラム有り
不可能
対応アプリケーション転送要求パケット送出
S205
アプリケーション受信待ち
S206
S207
転送終了？
未終了
S212
規定時間超過？
未超過
例外処理
S213
異常終了
データ処理開始
S208
出力イメージ生成
S209
S210
不正
認証結果
正当
印字出力
S211
終了

【図６】


(a)
START
データパケット受信
S301
データ処理開始
S302
出力イメージ生成
S303
S304
登録ユーザー？
S305
印字出力
S306
ディスクにイメージ保存
終了
(b)
START
登録イメージの順次読み出し
S307
S308
イメージ有り？
S314
別データ読み出し
S313
有り
S309
ＩＤの確認
対応データ無し
不一致
S310
一致？
異常終了
一致
印字出力
S311
イメージ破棄
S312
終了

【図7】


START
登録イメージの順次読み出し
S315
S316
イメージ有？
無
有
S320
別イメージ読み出し
登録日付確認
S317
S318
未超過
規定時間超過？
超過
登録イメージの破棄
S319
終了